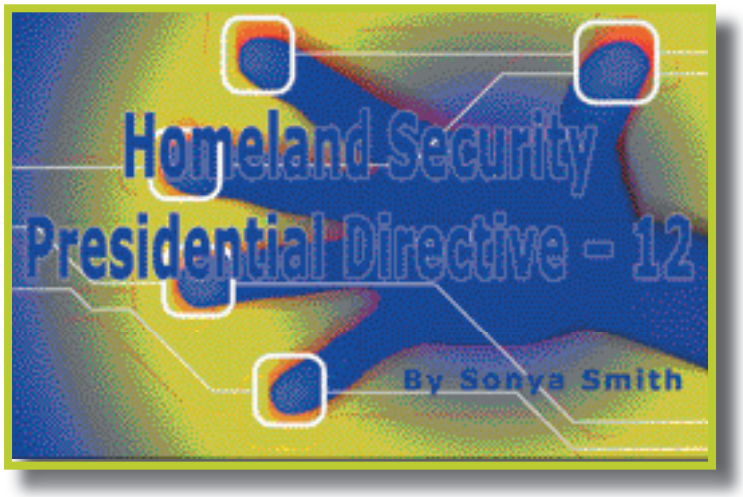

October 2006 marked the implementation date for issuing federal identification credentials in accordance with the Homeland Security Presidential Directive-12 (HSPD-12) standard …

President Bush signed HSPD-12 in August 2004; the directive sets a mandatory governmentwide standard for secure and reliable forms of identification for federal employees and contractors. HSPD-12 also requires the use of identification by federal employees and contractors that meets this standard in gaining physical access to federally controlled facilities and logical access to federally controlled information systems.

What this directive means for federal agencies is that they must use a secure and reliable identification that: (a) is based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting and terrorist exploitation; (c) is rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process.

The Department of Defense has a tremendous investment in the Common Access Card and the Public Key Infrastructure. Therefore, the CAC has been officially approved to be the DoD vehicle for HSPD-12 compliance. Changes are in store for the CAC and its issuance process to make it HSPD-12 compliant. Among other HSPD-12 required items, a contactless capability will be added using radio frequencies to transfer data between the card and the reader *(vice having to read the CAC's magnetic stripe or bar code)* and adding biometrics (a facial image and two electronic fingerprints) to the card.

The HSPD-12 compliant CAC will be phased in over time through 2010. The DoD has an initial operating capability solution at the Defense Manpower Data Center (DMDC) and will gradually deploy the capability throughout the Defense Department. Additional changes are on the horizon as the DoD pushes to maximize usage of the CAC. The Joint Task Force for Global Network Operations (JTF-GNO) Communications Tasking Order accelerated the implementation of PKI technology. This tasking order ties in perfectly with the HSPD-12 requirements and the Department's use of the CAC as a common identification standard for logical access.

The DoD now needs to establish the same type of momentum on the physical access side that the JTF-GNO Communications Tasking Order provided on the logical access side. Defense Department personnel are now using the CAC for applications that include digitally signing and encrypting e-mail, arranging travel, managing food service and tracking weapons issuance.

Reducing the number of different types of credentials issued, and using the CAC to its fullest potential as the standard physical access card will improve DoD's security posture and result in cost savings. Commands considering purchasing or upgrading physical access control systems (PACS), will need to verify whether the vendor is on the General Services Administration approved products list for HSPD-12 compliant products and services. They should also obtain a copy of the National Institute of Standards and Technology (NIST) certification to verify Federal Information Processing Standard (FIPS) 201-1 compliance before proceeding with any PACS purchases.

DMDC has produced a couple of key reference documents (see text box below) to assist: DoD CAC Middleware Requirements Release 3.0, Version 1.0 of 21 March 2006; and the DoD Implementation Guide for the NIST Special Publication 800-73, which defines the interfaces for personal identity verification.

However, commands considering the purchase of PACS should stay tuned. The DMDC currently has a pilot underway with all the military services to: (1) Test interoperability with existing Defense Department PACS; (2) Standardize at ISO 14443, Parts 1-4 at 13.56 Mhz; (3) Test the ability to read and interpret the HSPD-12 required card holder unique identifier; (4) Gain understanding of the impact of standardizing physical access control technology; and (5) Test interoperability with other federal sector departments and agencies. The reports from this pilot will be available next quarter.

One of the things that the DMDC discovered during the physical access pilot is that getting the middleware specifications correct is critical. The new middleware requirements must be defined for vendors to ensure they have the appropriate middleware to support HSPD-12 end state cards from any agency as well as the HSPD-12 compliant CACs.

The changes to the CAC to make it HSPD-12 compliant, such as the addition of contactless interface and biometrics, will bring much anticipated improved functionality to the CAC. Change is always difficult, but HSPD-12 promises a new era of interoperability between federal agencies.

Reference Documents to Help You Get Started

HSPD-12, Homeland Security Presidential Directive, August 27 2004, Policy for a Common Identification Standard for Federal Employees and Contractors: http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.

FIPS 201-1 Federal Information Processing Standard 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006: http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.

Government Approved Services and Products: http://idmanagement.gov/drilldown.cfm?action=gov_app_products.

DoD CAC Middleware Requirements Release 3.0, Version 1.0, March 21, 2006: http://www.dmdc.osd.mil/smartcard/owa/ShowPage?p=DevloperSupport.

DoD Implementation Guide for NIST Special Publication 800-73: http://www.dmdc.osd.mil/smartcard/owa/ShowPage?p=HSPD12.

Ms. Sonya Smith supports the DON CIO Information Assurance team. She can be reached at sonya.r.smith1.ctr@navy.mil. CHIPS